ENGINEERING FOR SAFETY OF CRITICAL INDUSTRIAL AND CIVIL

(Lecce - Università degli Studi)

Teaching DATA ENGINEERING AND SECURITY FOR CYBER PHYSICAL SYSTEMS

GenCod A007225

Owner professor TEODORO MONTANARO

Reference professors for teaching Lucio Tommaso DE PAOLIS, TEODORO MONTANARO

Teaching in italian DATA ENGINEERING AND SECURITY FOR CYBER PHYSICAL

Teaching DATA ENGINEERING AND SECURITY FOR CYBER PHYSICAL

SSD code IINF-05/A

Reference course ENGINEERING FOR SAFETY OF CRITICAL INDUSTRIAL AND

Course type Laurea Magistrale

Credits 9.0

Teaching hours Front activity hours: 81.0

For enrolled in 2026/2027

Taught in 2026/2027

Course year 1

Language ENGLISH

Curriculum INDUSTRIAL AND CIVIL INFRASTRUCTURES

Location Lecce

Semester First Semester

Exam type Oral

Assessment Final grade

Open **Course timetable**

BRIEF COURSE DESCRIPTION	Cyber-Physical Systems (CPS) integrate computational intelligence with physical processes, generating continuous streams of sensor data, telemetry, and control signals that must be collected, stored, and processed reliably before they can be trusted, analyzed, or defended. This course addresses both sides of that challenge: how to engineer the data infrastructure that CPS rely on, and how to secure the interconnected architectures that infrastructure supports, architectures whose security is critical for industrial, urban, and societal infrastructure, since a breach in a CPS can propagate from the cyber domain into the physical world, causing disruptions, equipment failures, or direct harm to people and environments. Students will first learn what CPS are and how they work, then follow the lifecycle of the data they produce, from ingestion and storage to processing, quality, and governance, before moving into the core security journey: identifying threats and vulnerabilities, and mastering the tools and methodologies needed to design, defend, and respond to attacks on these systems. Throughout, students will explore both theoretical frameworks and hands-on practical scenarios, developing the analytical mindset required of a modern data and security engineer working with critical infrastructure. Topics include: 1. CPS Foundation Cyber-Physical Systems: definitions, architectures, and technologies 2. CPS Protocols and Industrial Control Systems (SCADA, PLC, Modbus, etc.) 3. Data Engineering for CPS: ingestion, streaming vs. batch, storage (time-series databases, data lakes/warehouses), processing, data quality and governance 4. Data security and privacy in CPS pipelines 5. Security Engineering principles, threat modeling, and risk analysis 6. Network security: cryptography, TLS/SSL, VPNs, firewalls, IDS/IPS 7. Device and user protection: authentication, MFA, patch management, least privilege 8. Decentralized trust: DLT and Blockchain 9. IT management, standards, and compliance (ITIL, NIS2, ISO/IEC 27001, IEC 62443) and Digital Twins as a CPS/security architecture 10. Attack anatomy: Cyber Kill Chain and MITRE ATT&CK 11. Attack recognition and detection methods 12. Real-world CPS attack case studies 13. Incident Response and Resilience 14. Practical exercises
REQUIREMENTS	Basic knowledge about cyber-physical systems are welcome but not essential

COURSE AIMS	**Knowledge and understanding.** After completing the course, students will be able to: ▪ Describe and analyze the security posture of a Cyber-Physical System, identifying vulnerabilities at the network, device, data, and process levels. ▪ Design a basic data pipeline for CPS-generated data, selecting appropriate ingestion, storage, and processing approaches and justifying data quality and governance choices. ▪ Apply threat modeling frameworks (STRIDE, LINDDUN, DREAD, PASTA) to real-world CPS architectures, including data pipelines and Digital Twin components. ▪ Select and justify appropriate countermeasures for identified threats, including cryptographic protocols, network segmentation strategies, authentication mechanisms, and data protection controls. ▪ Interpret attack patterns using the Cyber Kill Chain and MITRE ATT&CK/D3FEND frameworks, and recognize Indicators of Compromise (IoC) and Indicators of Attack (IoA). ▪ Conduct a structured Incident Response process, from detection and containment through eradication, recovery, and post-incident analysis. ▪ Perform basic practical security assessments and data pipeline exercises on simulated CPS environments. **Making judgements.** Students are guided to critically evaluate data engineering and security scenarios, compare alternative solutions, and autonomously propose the most appropriate data architecture and defense strategies given the constraints of a specific CPS context, including safety-critical environments where data quality failures or security breaches may have physical consequences. **Communication.** Students will develop the ability to present and argue data architecture choices, security assessments, threat analyses, and proposed countermeasures clearly and rigorously, using domain-specific terminology appropriate to both technical and managerial audiences. **Learning skills.** The course fosters an investigative attitude toward emerging technologies, data infrastructures, and threats. Students will develop the habit of consulting authoritative resources (MITRE, CISA, NIST) and be prepared to continue learning independently as both the data engineering landscape and the threat landscape evolve.
TEACHING METHODOLOGY	The course combines frontal theoretical lectures with practical laboratory sessions. Theoretical lessons introduce concepts, frameworks, and methodologies progressively, building from CPS fundamentals through to advanced attack and defense techniques. Students are actively encouraged to participate, ask questions, and discuss real-world examples during class. Practical sessions complement the theory through direct engagement with security tools and simulated environments, including network reconnaissance with Kali Linux and guided exercises on the TryHackMe platform. Real attack case studies are analyzed to connect theoretical frameworks with documented historical incidents.
ASSESSMENT TYPE	The exam integrates practical and descriptive components.
OTHER USEFUL INFORMATION	*Office Hours* By appointment. Students may contact the instructor by email or directly at the end of class sessions.

FULL SYLLABUS

1. CPS Foundation Cyber-Physical Systems: definitions, architectures, and technologies
2. CPS Protocols and Industrial Control Systems (SCADA, PLC, Modbus, etc.)
3. Data Engineering for CPS: ingestion, streaming vs. batch, storage (time-series databases, data lakes/warehouses), processing, data quality and governance
4. Data security and privacy in CPS pipelines
5. Security Engineering principles, threat modeling, and risk analysis
6. Network security: cryptography, TLS/SSL, VPNs, firewalls, IDS/IPS
7. Device and user protection: authentication, MFA, patch management, least privilege
8. Decentralized trust: DLT and Blockchain
9. IT management, standards, and compliance (ITIL, NIS2, ISO/IEC 27001, IEC 62443) and Digital Twins as a CPS/security architecture
10. Attack anatomy: Cyber Kill Chain and MITRE ATT&CK
11. Attack recognition and detection methods
12. Real-world CPS attack case studies
13. Incident Response and Resilience
14. Practical exercises

REFERENCE TEXT BOOKS

The instructor provides teaching materials during the course and publishes them on the official academic e-learning solution (https://elearning.unisalento.it/).